

Necessità di indagine e tutele costituzionali fra mondo reale e mondo virtuale

Quando ho letto il titolo del Convegno, la mia prima reazione è stata di grande interesse, perché si tratta di un argomento importante ed attuale, ma anche di rinuncia: non sono esperto di captatori informatici o di una branca del diritto che richieda perquisizioni ed intercettazioni ambientali, per cui ho inizialmente pensato di lasciare il campo a chi ne sa più di me.

Visto però che sono anche un chiacchierone, alla fine ho ritenuto che, tutto sommato, non fosse neppure male proporre il punto di vista del comune cittadino, il quale si aspetta di essere tutelato dallo Stato e dalla legge. Sentirsi tutelato significa pretendere che non sia possibile che qualcuno butti giù la porta all'una di notte per portarti in un gulag senza motivo e senza processo, ma significa anche aspettarsi di poter fare una gita senza che nessuno metta una bomba sul treno o svuoti l'appartamento mentre ci si trova fuori casa.

E' un problema di punto di equilibrio: in uno Stato totalitario c'è scarsa criminalità comune, ma il primo criminale rischia di essere lo Stato stesso, che sopprime le libertà di espressione e la dignità degli individui. In uno Stato dove il garantismo sia portato all'estremo le forze dell'ordine e la magistratura risultano imbrigliate. Alla fine la gente non si sente tutelata e forze parallele a quelle dello Stato vanno a riempire il vuoto.

D'altra parte lo scopo di un convegno, non è (solo) quello di presentare risposte attraverso le conclusioni degli esperti, ma anche quello di suscitare il dibattito, di presentare punti di vista diversi, di porre domande.

Come mio solito, ho cercato di iniziare dalle origini. Credevo che le prime norme scritte di cui disponiamo fossero raccolte nel Codice di Hammurabi (ca. 1750 a.C.), invece il primato pare essere dei Sumeri, precisamente col Codice di Ur-Nammu, (ca. 2000 a.C.). Vediamo alcune norme in essi contenute:

Codice di Ur-Nammu

Omicidio

- 1. Se un uomo commette omicidio sia condannato a morte*

Rapina

- 2. Se un uomo commette rapina sia condannato a morte.*

Sequestro di persona

- 3. Se un uomo commette un sequestro sia condotto in carcere e condannato a pagare 15 sicli d'argento.*

Ma se il sequestrato moriva la condanna era la morte.

Falsa testimonianza

- 27. Se un uomo ha testimoniato il falso in un processo, sia condannato a pagare 15 sicli d'argento.*

Furto

Il ladro era condannato a pagare il doppio di quanto aveva rubato.

Se un funzionario pubblico veniva in possesso di uno schiavo, di un asino o di un bue perduti, non li restituiva subito e li tratteneva presso di sé per oltre un mese, veniva accusato di furto.

Violazione di domicilio

Chi si introduceva in una abitazione forzando la porta o facendo un buco nel muro veniva condannato a morte.

Se un uomo era trovato di giorno in un'abitazione veniva condannato a pagare 10 sicli. Di notte la pena diventava la morte.

Codice di Hammurabi

1. Qualora qualcuno accusi un altro, ponendo un bando su di lui, ma non possa provare l'accusa, allora quello che ha accusato sia messo a morte.

2. Qualora qualcuno abbia portato un'accusa contro un uomo, e l'accusato salti nel fiume, qualora egli affondi nel fiume l'accusatore prenda possesso della sua casa. Ma qualora il fiume provi che l'accusato non è colpevole, e qualora ne esca indenne, allora chi aveva portato l'accusa sia messo a morte, mentre chi era saltato nel fiume prenderà possesso della casa appartenuta all'accusatore.

3. Qualora qualcuno porti un'accusa di qualche crimine davanti agli anziani, e non provi ciò che ha denunciato, qualora si tratti di un crimine per cui è prevista la pena capitale, sia messo a morte.

5. Qualora un giudice esamini un caso, raggiunga una decisione, e presenti il suo giudizio per iscritto; qualora poi un appaia un errore nella sua decisione, e ciò dipenda da sua colpa, paghi allora dodici volte la multa da lui stabilita nel caso, e sia pubblicamente rimosso dal posto di giudice, né mai più vi sieda per rendere giustizia.

8. Qualora qualcuno rubi bestiame o pecore, o un asino, o un maiale o una capra, qualora esso appartenga a un dio o alla corte, il ladro paghi trenta volte tanto; qualora appartengano a un uomo liberato del re paghi egli il decuplo; qualora il ladro non abbia nulla con cui pagare, sia messo a morte.

E via così, con tante regole che riguardano la dote della sposa, l'adozione, il commercio. Pur se una serie di prescrizioni oggi ci fanno sorridere o ci appaiono assurde, se non accettiamo più la distinzione uomo/donna o libero/schiavo, è interessante notare che queste norme, molte della quali ancora più antiche poiché già in essere secondo un diritto consuetudinario trasmesso oralmente, rivelano che alcuni principi sono universali. Infatti si parla anche di legge naturale, che prevede che non si possa uccidere, non si possa rubare, non si possa entrare in casa d'altri.

Vi è una legge vera, ragione retta conforme alla natura, presente in tutti, invariabile, eterna, tale da richiamare con i suoi comandi al dovere, e da distogliere con i suoi divieti dall'agire male... A questa legge non è possibile si tolga valore né è lecito che in qualcosa si deroghi, né essa può essere abrogata; da questa legge non possiamo essere sciolti ad opera del senato o del popolo... Essa non è diversa a Roma o ad Atene, non è diversa ora o in futuro: tutti i popoli invece in ogni tempo saranno retti da quest'unica legge eterna e immutabile. (Cicerone, De re publica, I secolo a.C.)

Rivelano altresì che in ogni epoca c'è stato chi è andato contro questi principi, che ci si aspetta una tutela da parte dello Stato, che chi ha commesso il reato si ritiene debba subire una punizione. Che il codice sumero sia più rivolto all'indennizzo, mentre quello di Hammurabi sia più orientato alla vendetta e preveda la legge del taglione (addirittura statuisce che in alcuni casi anziché il colpevole venga ucciso suo figlio)¹ è altra questione, ma il principio violazione/sanzione è congenito. Come naturale pare essere il principio di uguaglianza, ovvero la necessità che due reati uguali siano puniti nello stesso modo, da cui deriva l'esigenza di norme scritte che diano uniformità di giudizio e di castigo. Interessante anche notare come già all'epoca doveva esserci chi abusava del diritto, per cui, pur in assenza di un Codice di Procedura, era previsto l'onere della prova ed una punizione per chi denunciava un reato senza essere in grado di provarlo o che fosse prevista una responsabilità del giudice e la forma scritta. Anche il fatto che ci possano essere errori giudiziari o abusi del diritto pare essere un principio naturale.

Notiamo come anche quelle civiltà note per essere violente e praticare il sacrificio umano, ad esempio i Maya, riconoscevano la legittimità dell'omicidio solo in circostanze specifiche o verso categorie definite, come i prigionieri di guerra, mentre prevedevano sanzioni per l'omicidio ingiustificato o il furto, che erano puniti rispettivamente con la morte e la schiavitù.

Con l'avvento dell'informatica non è cambiato nulla. O quasi. Visto che qui in sala ci sono alcuni dei migliori giuristi informatici d'Italia, potranno certamente fare delle precisazioni su alcune sottigliezze del reato informatico, parlarci delle problematiche relative all'individuazione del foro competente (se mi rubano il televisore esso ed il ladro si trovano in un luogo fisico ben preciso, se mi clonano la carta di credito la questione è molto più sfumata) ma per il cittadino comune non c'è nessuna differenza se gli viene rubato il portafoglio portando via delle banconote fisiche o viene violato il conto on-line portando via del denaro virtuale; per il commerciante non fa alcuna differenza se l'estorsione deriva dalla minaccia di bruciare il magazzino della merce o dal criptovirus che richiede un pagamento per sbloccare il computer aziendale.

Alcune innovazioni magari potranno portare ad una vera revisione del diritto, pensiamo ad esempio alle auto senza guidatore. Per ora devono avere un patentato a bordo, che sarà responsabile di eventuali incidenti, ma quando saranno completamente autonome, in caso di sinistro con torto, chi sarà il responsabile? Il proprietario? Il costruttore? Il programmatore? O si deciderà che in questi casi scompare l'aspetto penale, per quanto anche l'aspetto assicurativo crei alcuni problemi², e ci si limiterà ad un risarcimento del danno, oppure sarà difficile ricondurre l'episodio nell'ambito di una situazione di diritto esistente anziché creare nuovi principi giuridici, anche perché mi è stato insegnato che soggetto di diritto è un centro di interessi, ed un robot non ha interessi, a parte quello dell'alimentazione elettrica, e non è pertanto imputabile. I reati informatici, invece, pur con tutte le varie tipicità e difficoltà procedurali, possono normalmente essere ricondotti a nozioni esistenti. Anche quei reati specifici del mondo digitale, come l'accesso abusivo ai sistemi informatici³, in realtà reinterpretano in chiave moderna prescrizioni già in essere, ad esempio il divieto d'accesso ad archivi fisici⁴. A volte si è proposta una revisione

¹ 230. Qualora [il crollo di un'abitazione] uccida il figlio del proprietario il figlio di quel costruttore sarà messo a morte.

² http://www.repubblica.it/motori/sezioni/sicurezza/2015/09/03/news/auto_a_guida_autonoma_quanti_dubbi-121952273/

³ Art 615 ter Codice Civile

⁴ Ad esempio l'art. 37 D.P.R. 223/89 che vieta l'accesso agli uffici anagrafici ai non addetti.

costituzionale in chiave informatica. Potrà anche essere utile specificare meglio, ma in molti casi il non voler riconoscere che una norma si applica anche al mondo informatico è pretestuoso. Un esempio:

Costituzione della Repubblica Italiana, art. 14

Il domicilio è inviolabile.

Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale.

Gli accertamenti e le ispezioni per motivi di sanità e di incolumità pubblica o a fini economici e fiscali sono regolati da leggi speciali.

E' possibile sequestrare uno smartphone ed accedere ai dati? Forse oggi i Padri costituenti avrebbero scritto "il domicilio, fisico e digitale, è inviolabile" (questa l'ho copiata dall'Avvocato Blengino!). Ma davvero occorre questa precisazione o altre simili per stabilire che la mia mail elettronica deve essere inviolabile tanto quanto la vecchia busta cartacea? Resto dell'idea che, per la maggior parte dei casi e con i dovuti adattamenti, non ci sia molta differenza concettuale fra i reati classici e quelli informatici, e, di conseguenza, molta differenza concettuale nella necessità di indagine e di giudizio.

Mentre filosofia e religioni continuano ad interrogarsi, come avviene da secoli, sul problema del male, io lo considero un dato di fatto e passo direttamente alla fase successiva, ovvero il problema di contrastarlo. Fermo restando che certi comportamenti possono essere giudicati più o meno legittimi a seconda dei vincitori e del contesto storico (se l'Inghilterra avesse vinto la guerra d'indipendenza oggi studieremmo che a Boston alcuni terroristi organizzarono un attentato, mentre se avesse vinto l'Asse oggi i partigiani sarebbero ricordati come sabotatori), gli Stati devono organizzare un sistema di protezione che comporta indagini, interrogatori, verifiche, perquisizioni al fine di identificare il colpevole e raccogliere il materiale probatorio. Il che inevitabilmente comporta l'indagare anche chi si rivelerà totalmente estraneo; ma che, se onesto e trattato in modo corretto, dovrebbe essere ben contento di avere collaborato e di essere risultato innocente.

Finora tutto questo è stato considerato necessario, accettabile ed accettato dalla gente. Per arrivare qui sono salito su un aereo e per salire sono stato sottoposto ad un controllo insieme al mio bagaglio. L'ho accettato non solo come imposizione, neppure perché credo che "chi non ha nulla da nascondere non ha nulla da temere" stante il fatto che chi lo ha detto – Hitler – non è propriamente un modello di salvaguardia delle libertà costituzionali, ma perché è il prezzo che devo pagare per avere la tranquillità che il mio vicino di sedile non possa avere un coltello con cui ferirmi se impazzisce durante il viaggio, né una pistola per dirottarmi a Timbuctu. A volte si è detto che questi controlli sono totalmente inutili. Personalmente non sono d'accordo; si può dire che qualcosa possa sfuggire, e questo è scontato, si può affermare che siano meno efficaci di quanto si pensi, e questo può essere vero, si può temere che un gruppo terroristico organizzato abbia risorse tali da superare i normali controlli, e questo può essere ragionevole, ma il pazzo, il cane sciolto, l'emulatore possono essere contrastati da un minimo livello di controllo.

Posti di blocco sulle strade, intercettazioni telefoniche ed ambientali, perquisizioni personali hanno aiutato a combattere terrorismo, spaccio di droga, attività illecite in senso lato. Si potrà

discutere se sia il metodo migliore, si potrà valutare se, come per i controlli aeroportuali, le risorse impegnate siano proporzionali ai risultati ottenuti, ma il principio in sé che in alcuni casi siano misure legittime è sancito dalla Costituzione ed accettato dalla gente. Come è accettato e prescritto che vengano applicate con garanzie definite: presenza di un legale di fiducia, perquisizione ad opera di persona dello stesso sesso (anche se oramai neppure di questo si può essere sicuri!), ingresso in casa solo su mandato del Giudice...

Tutto ciò premesso, andiamo a vedere come tutto questo possa applicarsi al mondo virtuale. Come mia abitudine, parto da un esempio concreto: alcuni mesi fa dalle mie parti sono stati arrestati due ragazzi che, secondo l'accusa, reclutavano volontari per l'ISIS attraverso Internet. Uno lavorava presso una ditta per la quale avevo lavorato anch'io anni fa, l'altro frequentava la stessa scuola di mia cugina, anche se in una classe superiore. In comune avevano la caratteristica di essere ragazzi integrati, diligenti nel lavoro e nello studio, impegnati nel calcio e nelle normali attività di svago dei ragazzi nel tempo libero. Alcuni miei ex colleghi hanno riferito di essere convinti che si tratti di un errore, perché dal modo di comportarsi e rapportarsi nulla lasciava trasparire che quel compagno di lavoro fosse capace di qualcosa del genere. Appelliamoci al principio di innocenza e lasciamo che la giustizia segua il suo corso. Quello che mi preme sottolineare, però, al di là dell'innocenza o colpevolezza della persona specifica, è il fatto che ci siano persone "normali", che si comportano in modo ineccepibile nel mondo reale ma che diventano terroriste in quello virtuale.

Che poi tanto virtuale non è, dato che attraverso Internet si può rubare, ricattare, ma anche uccidere. E non sto pensando ai servizi di killeraggio, che comportano l'azione nel mondo fisico, ma ai suicidi di persone oggetto di cyber bullismo, oppure agli attacchi hacker a pacemaker, sistemi di trasporto, sistemi di produzione e trasmissione dell'energia.

Nei casi che ho descritto, pedinamenti, intercettazioni telefoniche o microspie ambientali non avrebbero probabilmente portato a nulla, e l'unico modo di scoprire il reato è quello di monitorare l'attività sul WEB. Il che ci porta ai captatori informatici, strumenti in grado di prendere il controllo, totale o parziale, di un apparecchio elettronico, consentendo ad un operatore remoto di visualizzare l'attività del browser, di ascoltare le chiamate accedendo alla sorgente, quindi prima che vengano criptate, di prelevare o inserire dei file, di trasformare lo smartphone in un microfono e/o videocamera e così via. Certo, un approccio molto invasivo. E magari anche inutile come prova in Tribunale, dato che a quel punto, col pieno controllo remoto dello strumento, si possono inviare mail fasulle, copiare file all'interno del dispositivo, navigare su siti giudicati compromettenti, creando ad arte le prove di un'attività sovversiva. Peralto anche nel mondo reale, se nel corso di una perquisizione viene trovata droga, si può sempre tentare di obiettare che è stata messa dalla polizia. Oppure l'inquirente potrebbe, accidentalmente o consapevolmente, alterare delle prove.

Mi rendo perfettamente conto che, riferendomi all'esempio che ho portato, fossi rimasto in quella ditta avrei conosciuto la persona, magari avremmo fatto amicizia, magari saremmo entrati in grande confidenza ed avrei quindi potuto essere intercettato mentre andavo a rivelare fatti personali. Magari lo sono oggi con altre persone con cui sono in contatto ora e sono sottoposte a sorveglianza. Personalmente sono disposto ad accollarmi il rischio, purché possa sempre credere nelle Istituzioni, nella possibilità di controllo democratico, nell'utilità dell'indagine. E pretendo anche che tutto ciò che non è un reato e non riguarda l'indagine non venga divulgato: se da un

controllo ambientale si scopre che l'amico con cui gioco a carte è in realtà il mio amante o che dormo con l'orsacchiotto deve restare assolutamente riservato.

Se poi succede che il sistema di hacking venga a suo volta hackerato, com'è successo di recente, questo fa parte dell'imponderabile, ma d'altra parte anche i faldoni dei Tribunali sono stati a volte smarriti, sottratti o divulgati. Si tratta di cercare di mettere in atto tutte le azioni possibili per prevenire questi inconvenienti, di sanzionare i responsabili, ma non è ragionevole che un rischio potenziale annulli l'attività investigativa e giudiziaria.

Per concludere, ritengo che uno strumento per controllare l'attività on-line al fine di prevenire – possibilmente – azioni criminose nonché perseguire quelle già commesse sia assolutamente auspicabile, oltre che legittimo. Esattamente come nel mondo reale la polizia è dotata di armi e strumenti per il mantenimento dell'ordine, l'espletamento delle indagini, la repressione del reato. Esattamente come in passato nuovi strumenti tecnologici, come i telefoni, sono entrati a far parte dei mezzi d'indagine e di prova. Se così non fosse tanto varrebbe chiudere del tutto gli apparati di forza pubblica ed il sistema giudiziario.

Con questo non intendo affermare che il captatore informatico sia l'unico strumento o il migliore, su questo ho premesso che non sono un esperto e lascio la valutazione a chi ne sa più di me. Non intendo neppure dire che sono favorevole ad un utilizzo massivo ed indiscriminato di strumenti di controllo. Sto affermando che il punto centrale non è lo strumento in sé, sul quale si può certamente discutere e che, come tutto, può essere migliorabile e migliorato, bensì il suo utilizzo. Se poi ci sono delle alternative più efficaci e meno invasive, ben vengano, così come sarebbero benvenuti aeroporti dove si possa salire sull'aereo in tranquillità senza passare ai raggi X, ma finché non si trova di meglio teniamo quello che c'è e che più o meno funziona.

Non abrogiamo un versetto né te lo facciamo dimenticare, senza dartene uno migliore o uguale. (Il Corano, Sura II, versetto 106)

Così, dando sfoggio di cultura coranica, mi sono anche esposto ad un controllo...

Neppure intendo dire che non debba esistere l'anonimato in rete. L'anonimato è invece importante sia per il cittadino, che può esprimersi in tutta libertà quanto per lo Stato, che può comprendere quale sia il reale pensiero della gente.

I punti chiave, a mio parere, per l'utilizzo di un captatore informatico o di un qualunque altro mezzo che porti a risultati analoghi sono:

Chi autorizza l'installazione? Chi controlla? Chi controlla i controllori? Cosa accade se si verificano abusi? Per quanto tempo vengono conservate le informazioni? Cosa avviene delle informazioni raccolte casualmente e non inerenti l'indagine?

Naturalmente mi aspetto anche che si tenga in gran conto il principio di proporzionalità: se nel mondo reale l'obiettivo dell'inquirente è trovare un deposito di merce contraffatta, probabilmente è sufficiente un GPS nell'auto senza andare ad installare microcamere nell'alloggio o mettere sotto controllo posta e telefoni. Analogamente nel mondo virtuale non è detto che si debba sempre installare un captatore che, almeno potenzialmente, faccia qualunque cosa, ma si dovranno adottare strumenti specifici che, nel rispetto degli obiettivi dell'indagine, abbiano la minore invasività possibile. Infine mi aspetto che, prima di intraprendere una qualunque azione a seguito

di un'attività giudicata sospetta, ci sia una verifica umana, data la tendenza dei computer a prendere fischi per fiaschi.

In sostanza, si tratta di stabilire un buon punto di equilibrio fra il rispetto dei diritti ed il contrasto alla criminalità. Ciò che viene ritenuto valido nel mondo reale dovrà quindi essere trasposto in quello virtuale.

Queste sono le riflessioni e le domande di un comune cittadino, mediamente informato e consapevole, e non di un giurista informatico o di un esperto di software di controllo. A loro il compito di dare le risposte più appropriate, o di spiegare quali siano le domande giuste, se quelle poste risulteranno inadeguate.